IN THE CLAIMS

Please amend the claims as follows:

Claim 1 (Original): A data processing method performed by a computer, comprising:

a first step for specifying a plurality of linear conversion candidates respectively satisfying a restriction on a circuit for realizing linear conversion;

a second step for specifying for each of said plurality of linear conversion candidates specified in said first step a minimum value of the number of zeros arisen in respective results of performing linear conversion restricted by the linear conversion candidates on a plurality of input data; and

a third step for specifying said linear conversion candidate wherein said minimum value specified in said second step becomes largest among said plurality of linear conversion candidates specified in said first step.

Claim 2 (Original): A data processing method as set forth in claim 1, wherein:

said first step specifies as said plurality of linear conversion candidates linear conversion which is a combination of a plurality of unit linear conversions wherein one of two zero regions in a replacing matrix is replaced by a conversion matrix; and

said second step specifies said minimum value for each of said linear conversion candidates obtained by giving a plurality of different matrixes as said conversion matrixes of said plurality of unit linear conversion.

Claim 3 (Original): A data processing method as set forth in claim 2, wherein:

the number of said plurality of unit linear conversion is M; and

said unit linear conversion is realized by calculation of a matrix of M by M.

Claim 4 (Original): A data processing method as set forth in claim 3, wherein said first step defines said linear conversion candidates by a formula (1) below by using conversion matrixes C_1, C_2, C_3 and C_4.

$$\begin{pmatrix} I + C_4C_3 + C_2C_1 + C_4C_3C_2C_1 + C_4C_1 & C_2 + C_4C_3C_2 + C_4 \\ C_3 + C_3C_2C_1 + C_1 & I + C_3C_2 \end{pmatrix} \quad \cdots (1)$$

Claim 5 (Original): A data processing method as set forth in claim 1, wherein

when said linear conversion is a linear conversion restricted in round function processing of common key block encryption, said second step performs said linear conversion on said input data obtained by performing nonlinear diffusion processing on a plain data.

Claim 6 (Original): A data processing method as set forth in claim 1, further comprising a fourth step for configuring a linear conversion circuit having a circuit block for realizing said unit linear conversion corresponding to said linear conversion candidates specified in said third step.

Claim 7 (Currently Amended): A computer-readable ~~medium~~ memory including a program to be executed by a computer, comprising:

a first procedure for specifying a plurality of linear conversion candidates respectively satisfying a restriction on a circuit for realizing linear conversion;

a second procedure for specifying for each of said plurality of linear conversion candidates specified in said first procedure a minimum value of the number of zeros arisen in

respective results of performing linear conversion restricted by the linear conversion candidates on a plurality of input data; and

a third procedure for specifying said linear conversion candidate wherein said minimum value specified in said second procedure becomes largest among said plurality of linear conversion candidates specified in said first procedure.

Claim 8 (Currently Amended): A computer-readable memory ~~medium~~ as set forth in claim 7, wherein:

said first procedure specifies as said plurality of linear conversion candidates linear conversion which is a combination of a plurality of unit linear conversions wherein one of two zero regions in a replacing matrix is replaced by a conversion matrix; and

said second procedure specifies said minimum value for each of said linear conversion candidates obtained by giving a plurality of different matrixes as said conversion matrixes of said plurality of unit linear conversion.

Claim 9 (Previously Presented): A data processing apparatus, comprising:

a processor configured to specify a plurality of linear conversion candidates respectively satisfying a restriction on a circuit for realizing linear conversion;

a processor configured to specify for each of said plurality of linear conversion candidates a minimum value of the number of zeros arisen in respective results of performing linear conversion restricted by the linear conversion candidates on a plurality of input data; and

a processor configured to specify said linear conversion candidate wherein said minimum value becomes largest among said plurality of linear conversion candidates.

Claims 10-12 (Canceled).